AUTHENTICATED
U.S. GOVERNMENT
INFORMATION
GPO

§ 1311.30 Requirements for storing and using a private key for digitally signing orders.

(a) Only the certificate holder may access or use his or her digital certificate and private key.

(b) The certificate holder must provide FIPS-approved secure storage for the private key, as discussed by FIPS 140–2, 180–2, 186–2, and accompanying change notices and annexes, as incorporated by reference in § 1311.08.

(c) A certificate holder must ensure that no one else uses the private key. While the private key is activated, the certificate holder must prevent unauthorized use of that private key.

(d) A certificate holder must not make back-up copies of the private key.

(e) The certificate holder must report the loss, theft, or compromise of the private key or the password, via a revocation request, to the Certification Authority within 24 hours of substantiation of the loss, theft, or compromise. Upon receipt and verification of a signed revocation request, the Certification Authority will revoke the certificate. The certificate holder must apply for a new certificate under the requirements of § 1311.25.

§ 1311.35 Number of CSOS digital certificates needed.

A purchaser of Schedule I and II controlled substances must obtain a separate CSOS certificate for each registered location for which the purchaser will order these controlled substances.

§ 1311.40 Renewal of CSOS digital certificates.

(a) A CSOS certificate holder must generate a new key pair and obtain a new CSOS digital certificate when the registrant's DEA registration expires or whenever the information on which the certificate is based changes. This information includes the registered name and address, the subscriber's name, and the schedules the registrant is authorized to handle. A CSOS certificate will expire on the date on which the DEA registration on which the certificate is based expires.

(b) The Certification Authority will notify each CSOS certificate holder 45 days in advance of the expiration of the certificate holder's CSOS digital certificate.

(c) If a CSOS certificate holder applies for a renewal before the certificate expires, the certificate holder may renew electronically twice. For every third renewal, the CSOS certificate holder must submit a new application and documentation, as provided in § 1311.25.

(d) If a CSOS certificate expires before the holder applies for a renewal, the certificate holder must submit a new application and documentation, as provided in § 1311.25.

§ 1311.45 Requirements for registrants that allow powers of attorney to obtain CSOS digital certificates under their DEA registration.

(a) A registrant that grants power of attorney must report to the DEA Certification Authority within 6 hours of either of the following (advance notice may be provided, where applicable):

(1) The person with power of attorney has left the employ of the institution.

(2) The person with power of attorney has had his or her privileges revoked.

(b) A registrant must maintain a record that lists each person granted power of attorney to sign controlled substances orders.

§ 1311.50 Requirements for recipients of digitally signed orders.

(a) The recipient of a digitally signed order must do the following before filling the order:

(1) Verify the integrity of the signature and the order by having the system validate the order.

(2) Verify that the certificate holder's CSOS digital certificate has not expired by checking the expiration date against the date the order was signed.

(3) Check the validity of the certificate holder's certificate by checking the Certificate Revocation List.

(4) Check the certificate extension data to determine whether the sender has the authority to order the controlled substance.

(b) A recipient may cache Certificate Revocation Lists for use until they expire.